CLAIMS

What is claimed is:

1. A method for processing Common Transport Information Units in a Fibre Channel network having a first network entity and a second network entity, the method comprising:

receiving a Common Transport Information Unit at a first network entity from a second network entity in a Fibre Channel network;

identifying a security control indicator in the Common Transport Information Unit from the second network entity;

determining that a security association identifier associated with the Common Transport Information Unit corresponds to an entry in a security database; and

decrypting at least a first portion of the Common Transport Information Unit by using algorithm information contained in the entry in the security database.

2. The method of claim 1, wherein the entry in the security database was created after a Fibre Channel authentication protocol was executed between the first and second network entities.

3. The method of claim 1, wherein the first portion is decrypted using a key contained in the entry in the security database.

4. The method of claim 1, wherein the first portion is encrypted using an encryption algorithm selected from the group consisting of DES, 3DES and AES.

5. The method of claim 1, further comprising:

recognizing that an authentication hash block of the Common Transport Information Unit supports authentication as well as confidentiality; and

using algorithm information contained in the entry in the security database to authenticate the payload of the Common Transport Information Unit.

6. The method of claim 1, wherein the first and second network entities are selected from the group consisting of domain controllers, N_Ports or FC_Ports.

7. A method for transmitting encrypted Common Transport Information Units in a Fibre Channel network having a first network entity and a second network entity, the method comprising:

identifying a Common Transport Information Unit having a source corresponding to the first network entity and a destination corresponding to the second network entity;

determining if the Common Transport Information Unit corresponds to selectors of an entry in a security database;

encrypting a first portion of the Common Transport Information Unit using key and algorithm information associated with the entry in the security database; and

transmitting the Common Transport Information Unit to the second network entity.

8. The method of claim 7, wherein the entry in the security database was created after a Fibre Channel authentication protocol was executed between the first and second network entities.

9. The method of claim 7, wherein the Common Transport Information Unit carries an Extended CT_IU preamble and is confidentiality protected by encryption of the CT_IU payload.

10. The method of claim 7, wherein a first portion of the Common Transport Information Unit is encrypted using an encryption algorithm selected from the group consisting of DES, 3DES and AES.

11. The method of claim 9, wherein parameters in the Extended CT_IU preamble or in a Basic CT_IU preamble are protected for confidentiality.

12. The method of claim 11, wherein a CT_IU payload is padded prior to encrypting the first portion of the Common Transport Information Unit.

13. An apparatus for transmitting encrypted Common Transport Information Units in a Fibre Channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying a Common Transport Information Unit having a source corresponding to the first network entity and a destination corresponding to the second network entity;

means for determining if the Common Transport Information Unit corresponds to selectors of an entry in a security database;

means for encrypting a portion of the Common Transport Information Unit using key and algorithm information associated with the entry in the security database; and

means for transmitting the encrypted Common Transport Information Unit to the second network entity.

14. The apparatus of claim 13, wherein the entry in the security database was created after a Fibre Channel authentication protocol was executed between the first and second network entities.

15. An apparatus for receiving encrypted Common Transport Information Units in a Fibre Channel network having a first network entity and a second network entity, the apparatus comprising:

means for identifying that the Common Transport Information Unit has been secured;

means for looking up security parameters in a security database, thereby allowing the de-encapsulation of the Common Transport Information Unit;

means for decrypting an encrypted Common Transport Information Unit; and

means for verifying that an encrypted message has been sent by a purported sender and that the encrypted message has not been tampered during its transmission.

16. A computer program embodied in a machine-readable medium for processing Common Transport Information Units in a Fibre Channel

network, the computer program controlling a first network device to perform the following steps:

receive a Common Transport Information Unit from a second network device in the Fibre Channel network;

identify a security control indicator in the Common Transport Information Unit;

determine that a security association identifier associated with the Common Transport Information Unit corresponds to an entry in a security database; and

decrypt at least a first portion of the Common Transport Information Unit by using algorithm information contained in the entry in the security database.

17. A computer program embodied in a machine-readable medium for processing Common Transport Information Units in a Fibre Channel network, the computer program controlling a first network device to perform the following steps:

set a security control indicator in a Common Transport Information Unit;

set a security association identifier associated with the Common Transport Information Unit corresponding to an entry in a security database;

encrypt at least a first portion of the Common Transport Information Unit by using algorithm information contained in the entry in the security database; and

send the Common Transport Information Unit to a second network device in the Fibre Channel network.

18. A network device for receiving encrypted Common Transport Information Units in a Fibre Channel network, the network device comprising:

a plurality of ports for communication with other network devices in the Fibre Channel network; and

at least one processor configured to perform the following steps:

receive a Common Transport Information Unit from a second network device in the Fibre Channel network;

identify a security control indicator in the Common Transport Information Unit;

determine that a security association identifier associated with the Common Transport Information Unit corresponds to an entry in a security database; and

decrypt at least a first portion of the Common Transport Information Unit by using algorithm information contained in the entry in the security database.

19. A network device for sending encrypted Common Transport Information Units in a Fibre Channel network, the network device comprising:

a plurality of ports for communication with other network devices in the Fibre Channel network; and

at least one processor configured to perform the following steps:

set a security control indicator in a Common Transport Information Unit;

set a security association identifier associated with the Common Transport Information Unit corresponding to an entry in a security database;

encrypt at least a first portion of the Common Transport Information Unit by using algorithm information contained in the entry in the security database; and

send the Common Transport Information Unit to a second network device in the Fibre Channel network.